CLAIMS

What is claimed is:

1. A certification method, comprising the steps of:

acquiring a chain of linked certificates extending from a first entity, through at least one intermediate entity, to a second entity, the chain of linked certificates including a certificate signed by the intermediate entity vouching for predetermined information associated with the second entity; and

generating, from the chain of linked certificates, a collapsed certificate signed by the first entity vouching for the predetermined information associated with the second entity and including an identification of the at least one intermediate entity.

2. The method of claim 1 wherein the predetermined information associated with the second entity includes a public key of the second entity.

3. The method of claim 1 wherein each of the first entity and the at least one intermediate entity comprises a respective certification authority.

4. The method of claim 3 wherein the identification of the at least one intermediate entity includes indications of a name and a key associated with the respective certification authority.

ATTORNEY DOCKET NO. P4097
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

5. The method of claim 4 wherein the indication of the key associated with the respective certification authority comprises a digest of the key.

6. The method of claim 3 wherein the collapsed certificate further includes an identification of the first entity.

7. The method of claim 6 wherein the identification of the first entity includes indications of a name and a key associated with the respective certification authority.

8. The method of claim 1 wherein the collapsed certificate further includes a digest of the collapsed certificate.

9. The method of claim 1 wherein the identification of the intermediate entity includes an indication of a name associated with the intermediate entity.

10. The method of claim 1 wherein the first entity signs the collapsed certificate using a digital signature.

11. The method of claim 1 further including the step of providing the collapsed certificate directly to an entity requesting the certificate.

12. A method of determining whether access to a resource at a first node in a computer network should be granted to a client at a second node in the network in response

to a request for access to the resource by the client, the method comprising the steps of:

receiving the request for access to the resource at the first node from the client at the second node, the request including a collapsed certificate signed by a first certification authority vouching for predetermined information of the client and including an identification of an intermediate certification authority that vouches for the client's predetermined information;

determining whether the identification of the intermediate certification authority matches an identifier contained in a certificate revocation list; and

in the event the identification of the intermediate certification authority matches an identifier contained in the certificate revocation list, receiving an indication at the first node that a certificate for the intermediate certification authority has been revoked and denying the client access to the resource.

13. The method of claim 12 further including the step of verifying the authenticity of the request using a digital signature of the first certification authority.

14. A system for generating a collapsed certificate, the system comprising:

a memory including a computer program for acquiring a chain of linked certificates and for generating a collapsed certificate based on the respective linked certificates in the chain; and

a processor operative to execute the computer program,

the computer program including program code for:

acquiring the chain of linked certificates extending from a first entity, through at least one intermediate entity, to a second entity, the chain of linked certificates including a certificate signed by the intermediate entity vouching for predetermined information of the second entity; and

generating, from the chain of linked certificates, the collapsed certificate signed by the first entity vouching for the predetermined information of the second entity and including an identification of the at least one intermediate entity.

15. The system of claim 14 wherein each of the first entity and the at least one intermediate entity comprises a respective certification authority.

16. A system for determining whether access to a resource at a first node in a computer network should be granted to a client at a second node in the network in response to a request for access to the resource by the client, the system comprising:

a server operative to:

receive the request for access to the resource at the first node from the client at the second node, the request including a collapsed certificate signed by a first certification authority vouching for predetermined information of the client and including an identification

of an intermediate certification authority that vouches for the client's predetermined information;

determine whether the identification of the intermediate certification authority matches an identifier contained in a certificate revocation list; and

in the event the identification of the intermediate certification authority matches an identifier contained in the certificate revocation list, receive an indication at the first node that a certificate for the intermediate certification authority has been revoked and deny the client access to the resource.

17. The system of claim 16 wherein the server is further operative to verify the authenticity of the request using a digital signature of the first certification authority.

18. A computer program product including a computer readable medium, the computer readable medium having a computer program stored thereon for generating a collapsed certificate, the computer program being executable by a processor and comprising:

program code operative to:

acquire a chain of linked certificates extending from a first entity, through at least one intermediate entity, to a second entity, the chain of linked certificates including a certificate signed by the intermediate entity vouching for predetermined information of the second entity; and

generate, from the chain of linked certificates, a collapsed certificate signed by the first entity vouching for the predetermined information of the second entity and including an identification of the at least one intermediate entity.

19. The computer program product of claim 18 wherein the program code is further operative to provide the collapsed certificate directly to an entity requesting the certificate.

20. A computer data signal, the computer data signal including a computer program for use in generating a collapsed certificate, the computer program comprising:

program code operative to:

acquire a chain of linked certificates extending from a first entity, through at least one intermediate entity, to a second entity, the chain of linked certificates including a certificate signed by the intermediate entity vouching for predetermined information of the second entity; and

generate, from the chain of linked certificates, a collapsed certificate signed by the first entity vouching for the predetermined information of the second entity and including an identification of the at least one intermediate entity.

21. The computer data signal of claim 20 wherein the program code is further operative to provide the

collapsed certificate directly to an entity requesting the certificate.

22. An apparatus for generating a collapsed certificate, comprising:

means for acquiring a chain of linked certificates extending from a first entity, through at least one intermediate entity, to a second entity, the chain of linked certificates including a certificate signed by the intermediate entity vouching for predetermined information of the second entity; and

means for generating, from the chain of linked certificates, a collapsed certificate signed by the first entity vouching for the predetermined information of the second entity and including an identification of the at least one intermediate entity.

23. The apparatus of claim 22 further including means for providing the collapsed certificate directly to an entity requesting the certificate.